Information Assurance Security Awareness Brief

Marine Corps Recruiting Command

Instructions

- **Per MARADMIN 541/05, all personnel with USMC accounts must receive this Information Assurance (IA) training NLT 29 Nov 2005.**
- **Instructions for reporting completion of this training are provided at the end the presentation**
- **Per the MARADMIN, accounts for personnel who do not complete this training by 29 Nov 2005 will be disabled. This includes personnel who are TAD or on leave.**
  - MCRC Personnel whose accounts are disabled must contact their ISC or MCRC Help Desk to receive the training.
  - When training has been completed the account will be re-enabled.

What is Information Assurance?

- **Information operations that protect and defend information and information systems be ensuring their availability, integrity, authentication, confidentiality and non-repudiation… providing for restoration of information systems by incorporating protection, detection, and reaction capabilities.” CNSSI 4009**

Why IA's Important

- **Making sure the computer and the information is there when we need it (Availability).**
- **Making sure the information we use, transmit, process, or stored has not been corrupted or adversely manipulated (Integrity).**
- **Making sure we know who is using our computers and accessing our data (Authentication).**
- **Making sure the information is protected from disclosure (Confidentiality).**
- **Information contained in e-mail or stored under a profile may be used in a court of law (Non-repudiation).**

Information Systems Security Program

- **Basic Requirement of the Computer Security Act of 1987 & DoDI 8500.2 to ensure all Federal and DoD personnel receive INFOSEC training:**
- **To:**
  - Assure operational continuity
  - Reduce security risks to acceptable levels
  - Comply with applicable laws and regulations

Information Classification

- **All information processed at MCRC is considered to be, at the lowest classification, SENSITIVE and must be treated as such.**
- **Guiding Reference OMB Circular A-130**

Login Banner

- **Read it!**
- **By clicking OK you acknowledge that:**
  - the information system you are using is for "Official Government Use Only"
  - your computer and all information it contains are subject to inspection
  - your actions are subject to continuous auditing

Identification and Authentication

- **Positive identity of user before access to network is granted:**
  - Access requests through supervisors, (USMC System Authorization Access Request Form)
  - User is assigned Logon ID, personal authenticator (USMC SAAR, Certification Test)
    - USMC SAAR (Modified DD Form 2875) – Available on C4/IA website.

Password Protection

- **Personal passwords must remain private**
  - Don’t write it down
  - Don’t type a password while others watch
  - Don’t tell it to anyone over the phone, even a system administrator
  - Don’t record password on-line or e-mail it
  - Don’t use easily guessed words
    - SemperFi! ,Marines, DevilDog1
  - 8 characters, alpha-numeric, special characters
    - h0M3rUn#
- **Ref: MARADMIN 089/03**

Better Than a Pass”word”

- **Use a pass phrase known only to you**
- **Seems to be gibberish**
- **Same rules apply**
  - 8 or more characters, alpha-numeric, special characters
- **Example: “My dog is named Spot and has one foot.”**
  - Md1Ns&h1ft!

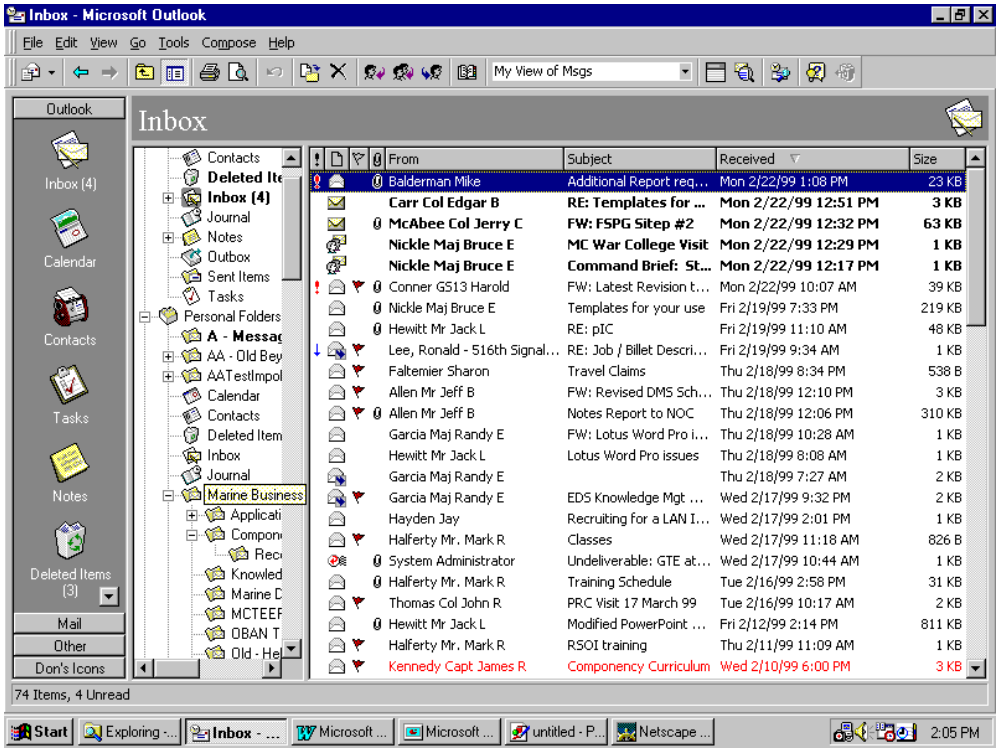
Remember:

- **Protect your username and password**
- **Use strong passwords**
- **Lock your computer when you step away**
- **Use your CAC to sign and encrypt sensitive email**

Appropriate Use of the Internet

- **Official Use**
- **Support USMC Mission**
- **Improve Professional Skills or Formal Academic Education**
- **Does not Adversely Affect Professional Duties**
- **Does NOT Adversely Reflect Upon The Corps**
- **Downloading any obscene or hate content is prohibited.**
- **<u>Every connection to the Internet is logged and reviewed</u>.**

E-mail/Policies



- **Chain Mail is not authorized to be forwarded. If in question do not send it.**
- **Only open Attachment (Files) from a trusted/known source. Scan all attachments with AntiVirus Software**

Use of Commercial E-Mail

- **Ref: CJCSM 6510.01 & MARADMIN 541/99**
- **Accessing commercial/web-based E-Mail services from MCEN not authorized**
  - Hotmail.com
  - AOL.com
  - Yahoo.com
- **Can RECEIVE or SEND messages from MCEN to commercial accounts**

E-Mail Policy (continued)

- **"UNDER NO CIRCUMSTANCES WILL OFFICIAL GOVERNMENT CORRESPONDENCE OR DATA FILES BE SENT OR FORWARDED TO, OR CREATED OR STORED ON, COMMERCIAL E-MAIL SERVICES. THIS INCLUDES, BUT IS NOT LIMITED TO, FORMAL MESSAGE TRAFFIC, WORKING DOCUMENTS AND PERSONAL OFFICIAL E-MAIL."**

Prohibited E-Mail Usage

- Illegal Activities
- Partisan Activity or Lobbying on Behalf of Organizations NOT Affiliated With the Corps or DoD
- Accessing, Storing, Displaying or Distributing Obscene Materials
- The Creation, Forwarding or Passing of Chain Mail

Audit (Monitoring)

- **All activity on the RSN Network is monitored to:**
  - Ensures system performance
  - Determine probable causes and impacts
  - Logs reviewed daily by authorized personnel.
  - E-Mail, Surfing Sites, etc. is ALL recorded somewhere.
  - **Read your logon warning banner**.

How Do Computer Viruses Spread?

- Email attachments (by opening them; if it is an executable file)
- Downloading files from the Internet
- Sharing software
- Commercial software
- Shareware/Freeware
- Third-party use of your computer

Anti-Virus Software

- **Computer viruses are a real threat to the RSN Network**
- **Virus definitions are updated automatically**
- **Anti-Virus software is available for HOME USE for all DOD personnel**
  - http://www.cert.mil/antivirus/symantec/sym-client-windows.htm
  - **Symantec Client Security 3.0.1 (Combined AV & FW Package)**
  - Download from a computer on .mil domain
- **Anti-spyware software is also available for DoD personnel**

Anti-Virus Software

- All media must be scanned for possible viruses when transferring files
- Do not disable auto-protect
- Home users are encouraged to scan their home PCs weekly and to acquire all virus signature updates when released

Viruses: What Do You Look For?

- **Note abnormal or unexpected activity**
  - Displays, music, or other sounds
  - Slowdown in processing speed
  - Disk activity
  - Error messages
  - Changes in file sizes
  - Loss of programs or data

If You Suspect an Infection

- **STOP processing**
- **Disconnect Network Cable from PC**
- **Scan all local, physical drives on your PC.**
- **Contact the MCRC Help Desk.**
- **If infected, wait for further instructions from the Help Desk**

Peer-to-Peer File Sharing

- **P2P poses a serious threat to the security and integrity of our networks**
- **Currently over 100 different P2P programs released**
- **Many P2P programs have built-in encryption and use dynamic port configuration, defeating firewall rule sets**
- **It has been discovered that there is a large presence of P2P programs on DoD networks to include healthcare facilities and operational units**

P2P Popularity

- **Peer to peer (P2P) file sharing applications (i.E. - KaZaA, Gnutella, Limewire, Grokster, Morpheus, etc) are exceptionally popular and used widely on the Internet.**
- **Many personnel are unaware of the security threats and potential legal ramifications associated with the use of these applications.**

P2P Threat

- **P2p applications provide means for the propagation of**
  - Viruses
  - Trojan horses
  - Other malware
- **How?**
  - data files transferred appear as music or video files
  - destructive viruses and Trojan horses are being camouflaged as these files
  - Allows for a more rapid and thorough propagation

Illegal Copies / Copyright

- **Many of the P2P exchanged files are illegal copies of music, video, or software programs which have been legally copyrighted or licensed by their owners.**
- **Transfer or ownership of these pirated files may result in legal or disciplinary action should the transferred file be acquired unlawfully.**
- **Opens up the Command to legal ramifications if pirated files are found on government-owned systems.**

P2P Serious Threat

- **Sensitive information leakage (OPSEC & Classified)**
- **Malicious Code (Viruses, Spyware, Backdoors)**
  - P2P programs often create a backdoor or back channel that can be manipulated by someone else.
- **Child pornography (P2P programs often used to trade child porn)**
- **Surreptitious data exfiltration of passwords, sensitive unclassified, or private information, leading to other intrusions and violations.**
- **Distributed Denial of Service (DDoS) attacks on DoD or other networks from DoD/USMC computers**

Incident Reporting

- **Report any unusual or suspicious activity**
  - Attempting unauthorized access
  - Abuse of authorized privileges
  - Use of privately-owned or unapproved software
  - Violation of copyright laws
  - Deliberate introduction of VIRUSES
  - Forwarding or Creation of CHAIN MAIL

User Responsibilities

- **Protect sensitive information**
- **Use Government AIS & Software for authorized use only**
- **Report suspected compromises**
- **<u>DO NOT</u> try to bypass Security Settings**

New User Agreement

- **Complete the New USMC User Agreement**
- **Command IAM will maintain on file**

FOR MORE INFORMATION:

Contact MCRC G-6 HelpDesk at 784-9420/21/22

References

- DoDD 8100.2
- CJCSM 6510.01
- MARADMIN 541/05
- MARADMIN 162/00, INFORMATION ASSURANCE BULLETIN 2-00
- MARADMIN 089/03
- ASD/NII Memo 13 Apr 2004, Elimination of Unauthorized Peer-to-Peer (P2P) File-sharing Applications Across DoD
- MARADMIN 541/99
- DISA IA Awareness Training